(Under) Investment in cyber skills and data protection enforcement

Evidence from the UK Information Commissioner's Office activity logs

Pantelis Koutroumpis Farshad Ravashan Taheya Tarannum

Oxford Martin School

August, 2023

In one internet minute ...

In one evil internet minute ...

Forbes

CYBERSECURITY • EDITORS' PICK

60 Seconds In Cybersecurity: Here's What Happens In Just One Malicious Internet Minute

Davey Winder Senior Contributor ⓘ
Co-founder, Straight Talking Cyber

Aug 27, 2020, 03:09am EDT

- 375 new cybersecurity threats will emerge.
- 16,172 records will be compromised.
- $1.63 million will be lost.

Motivation

An agency problem

- Cyber attacks often cause data breaches: Loss of personal data for customers but low direct costs for firms.
- Leads firms to underinvest in cyber security.
  (Kankanhalli et al., 2003; Gordon et al., 2015a,b; Kopp et al., 2017; De Cornière and Taylor, 2021; Bana et al., 2021)

Motivation

An agency problem

- Cyber attacks often cause data breaches: Loss of personal data for customers but low direct costs for firms.
- Leads firms to underinvest in cyber security. *(Kankanhalli et al., 2003; Gordon et al., 2015a,b; Kopp et al., 2017; De Cornière and Taylor, 2021; Bana et al., 2021)*

An institutional factor

- Data protection regulation and laws are crucial for internalizing the social costs of cyber attacks into firms' private costs.

Motivation

An agency problem

- Cyber attacks often cause data breaches: Loss of personal data for customers but low direct costs for firms.
- Leads firms to underinvest in cyber security. *(Kankanhalli et al., 2003; Gordon et al., 2015a,b; Kopp et al., 2017; De Cornière and Taylor, 2021; Bana et al., 2021)*

An institutional factor

- Data protection regulation and laws are crucial for internalizing the social costs of cyber attacks into firms' private costs.

Research question

- Does stronger data protection alleviate the effects of these misaligned incentives? We address this question by examining the effect on firms' cybersecurity hiring

This Paper

Temporal variation

- We Study two legal changes in data protection regulations in the UK that enforced by Information Commissioners' Office (ICO)
  - Change in law enforcement: Removal of requirement to prove 'substantial damage or distress (SDD)' in 2015.
  - Change in law content: Enactment of the DPA 2018 (UK-GDPR) that increased the ceiling of maximum monetary penalties.

This Paper

Temporal variation

- We Study two legal changes in data protection regulations in the UK that enforced by Information Commissioners' Office (ICO)
  - Change in law enforcement: Removal of requirement to prove 'substantial damage or distress (SDD)' in 2015.
  - Change in law content: Enactment of the DPA 2018 (UK-GDPR) that increased the ceiling of maximum monetary penalties.

Sectoral variation

- Novel data: Exploit ICO activity logs and supervisory actions to build an index for exposure to data protection enforcement

Our Findings

Quantitative effects: Data protection law is an effective device to incentivize firms to invest in cyber skills.

- 26% ↑ after the SDD removal.
- Up to 51% ↑ after the DPA 2018.

Our Findings

Quantitative effects: Data protection law is an effective device to incentivize firms to invest in cyber skills.

- 26% ↑ after the SDD removal.
- Up to 51% ↑ after the DPA 2018.

Qualitative effects: The response was stronger for

- Data-intensive firms
- Firms that invest in cloud
- Firms with ex-ante high cash holding

Our Findings

Quantitative effects: Data protection law is an effective device to incentivize firms to invest in cyber skills.

- 26% ↑ after the SDD removal.
- Up to 51% ↑ after the DPA 2018.

Qualitative effects: The response was stronger for

- Data-intensive firms
- Firms that invest in cloud
- Firms with ex-ante high cash holding

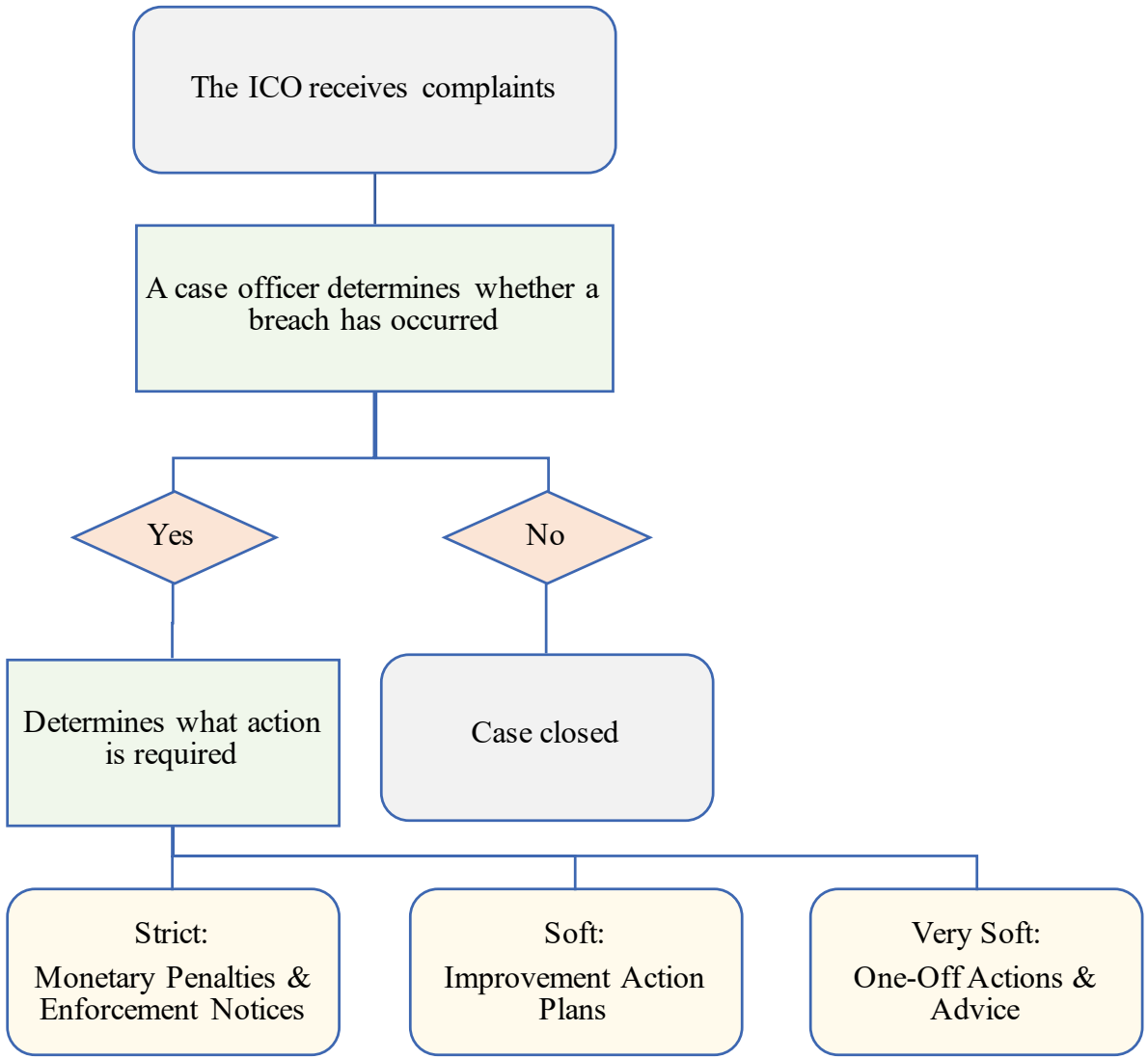
Economic trade-off: Slow down of firm dynamics; 12% ↓ in firm entry and 10% ↓ in firm exit.

Overview

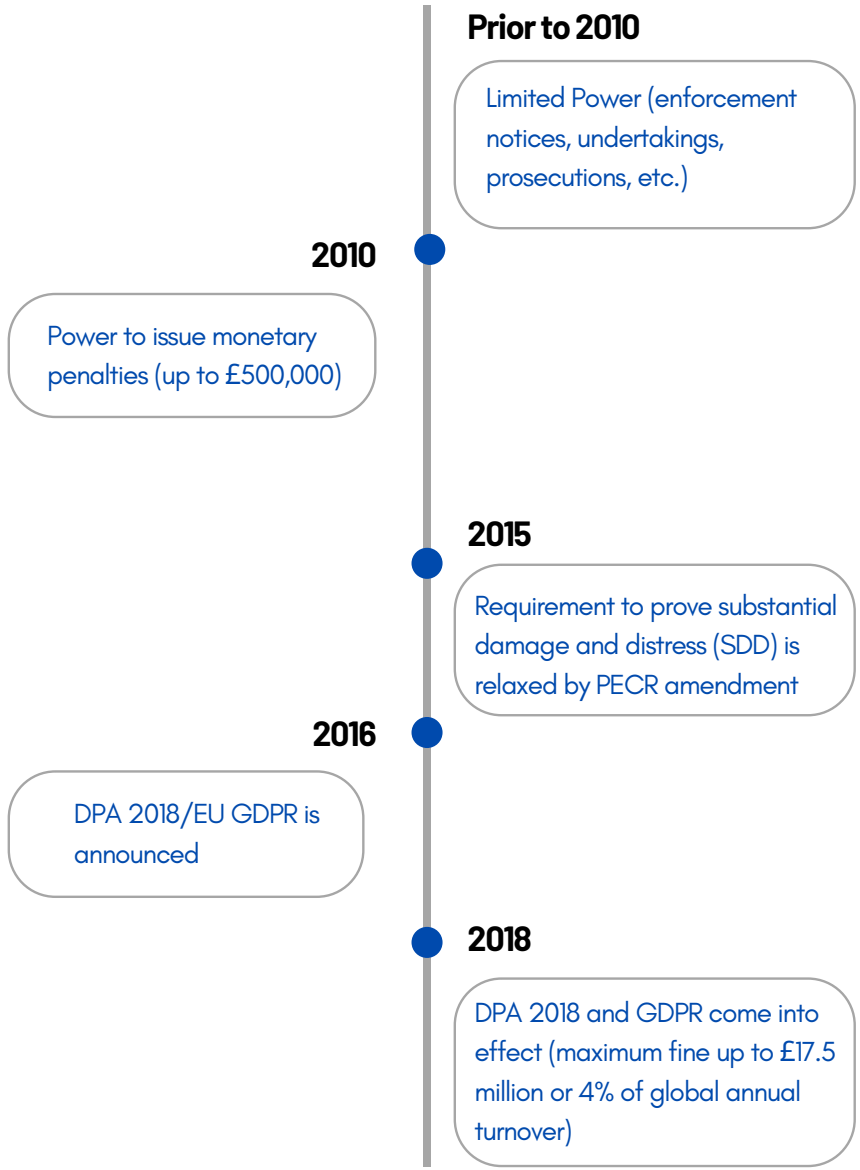
- Institutional set-up
  - UK Information Commissioner's Office
  - Legal status and institutional changes
- Empirical strategy
- Results
- Concluding remarks

Institutional Set-up

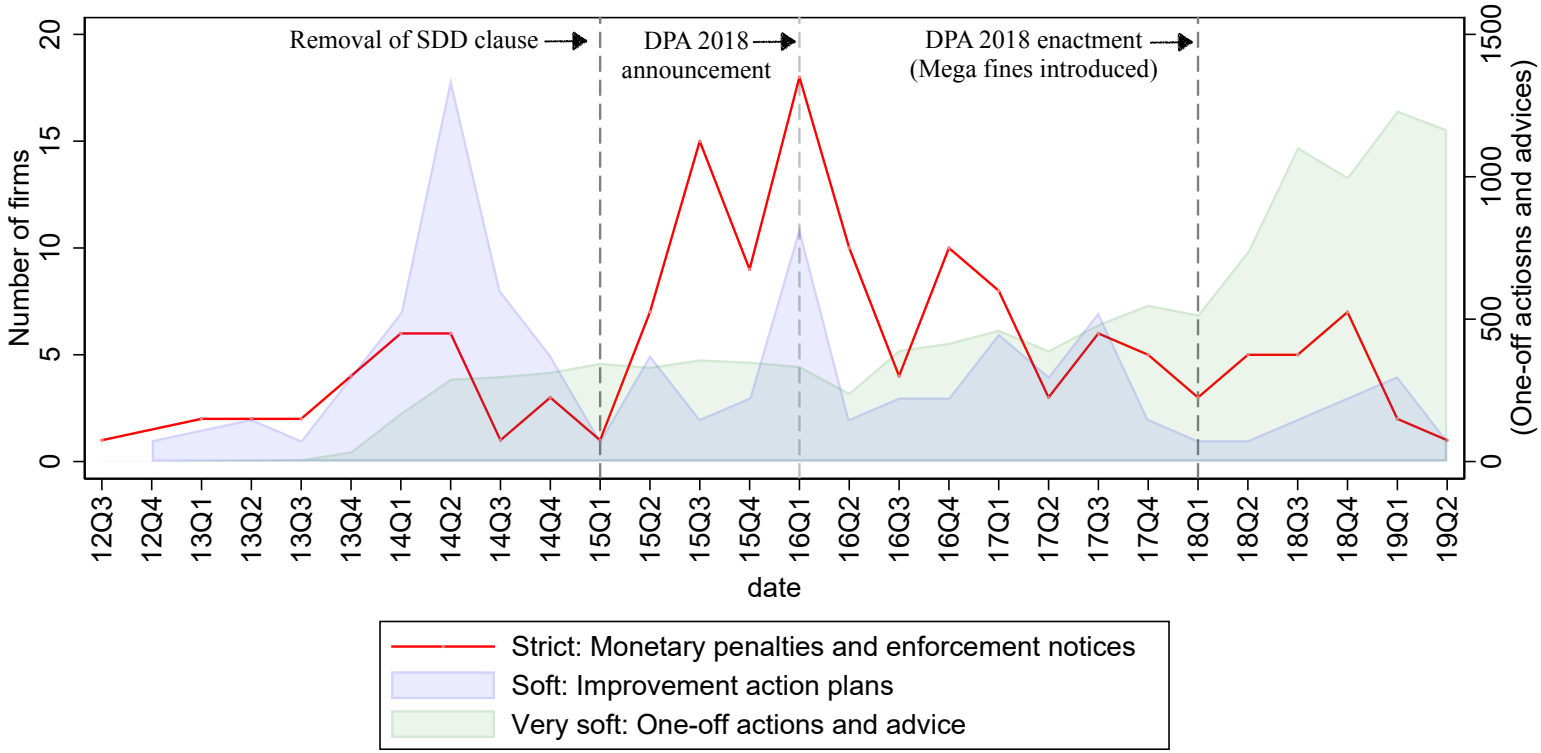
How ICO processes the complains



ICO Timeline



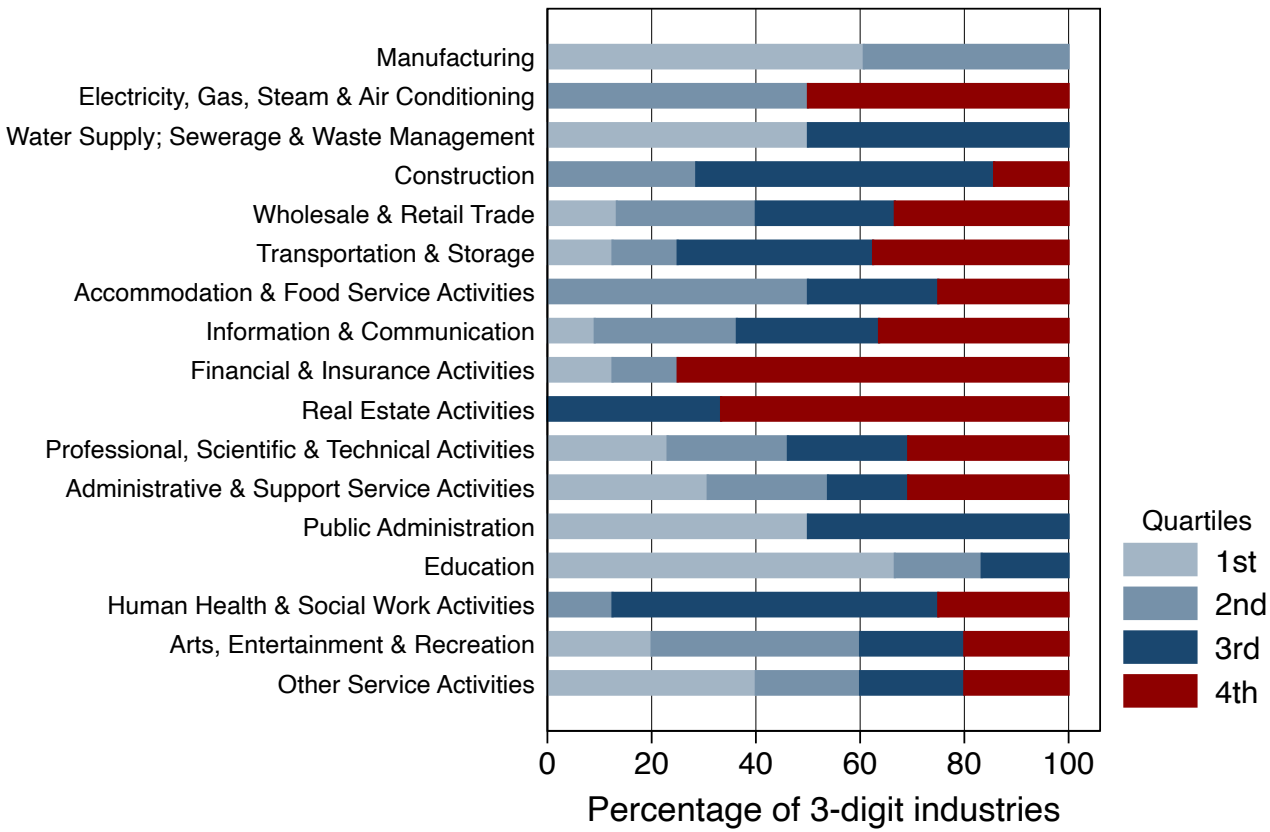
ICO enforcment trends



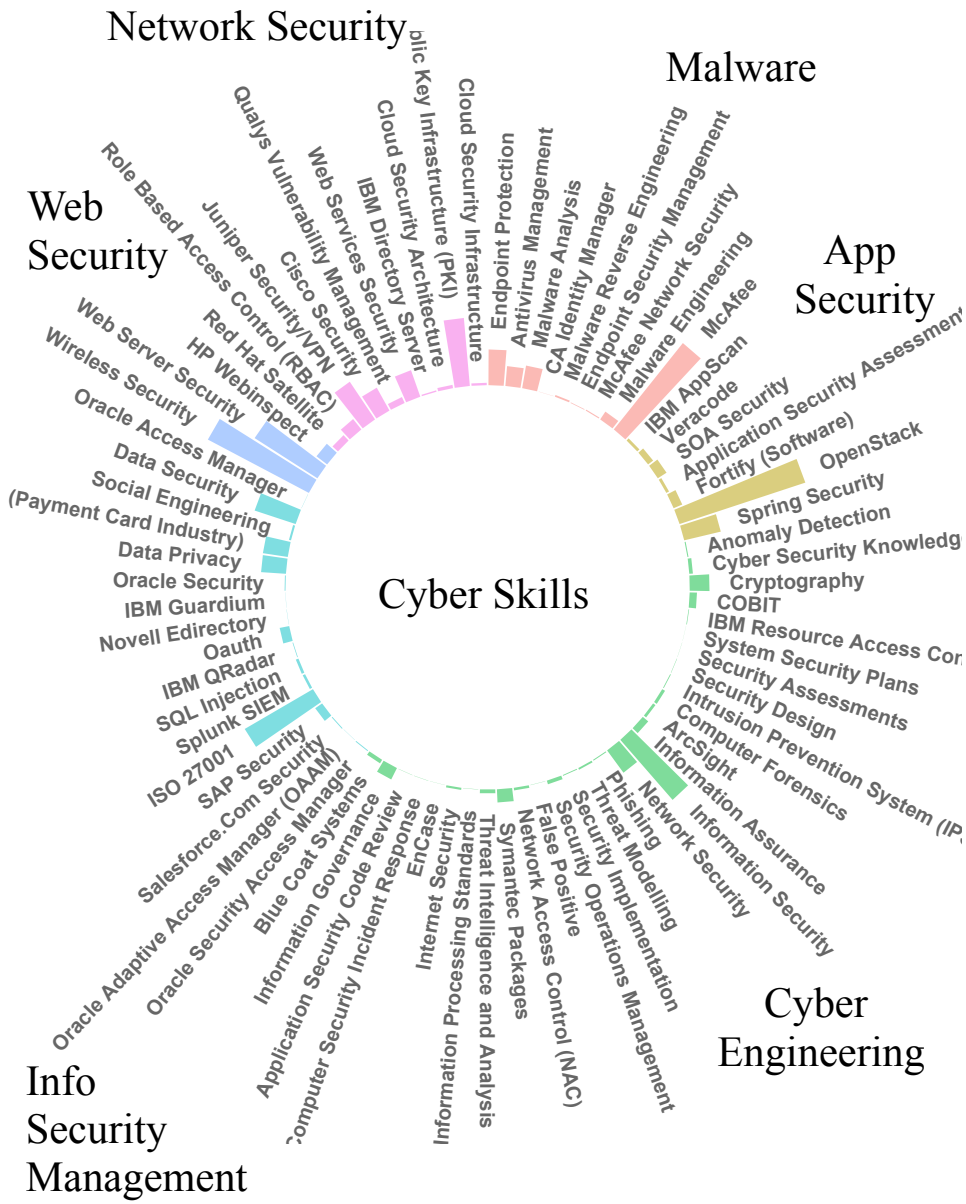
What we do in 4 slides

Measuring sectoral exposure to ICO enforcement (1/4)

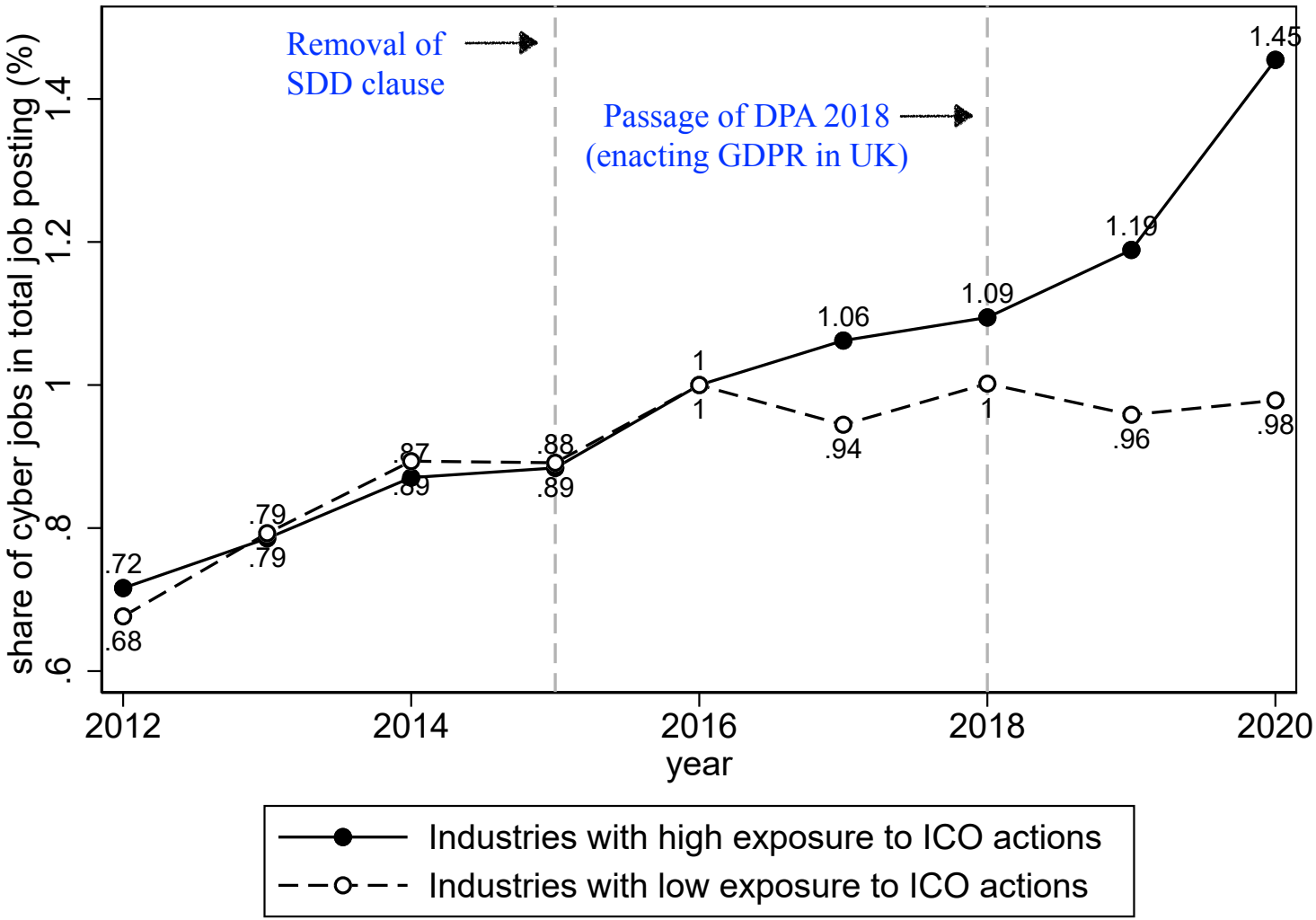
- Match with the UK business register to identify high vs. low exposure industries



Defining cyber skills from job postings data (2/4)



Using temporal variation of legal changes (3/4)



Empirical strategy (4/4)

TTWA-Level Analysis

$$cyber\_share_{cjt} = \beta_1 high\ ico\ exposure_j \times SDD_t + \beta_2 high\ ico\ exposure_j \times DPA_t + \delta_{ct} + \rho_{cj} + \epsilon_{cjt}$$

Firm-Level Analysis

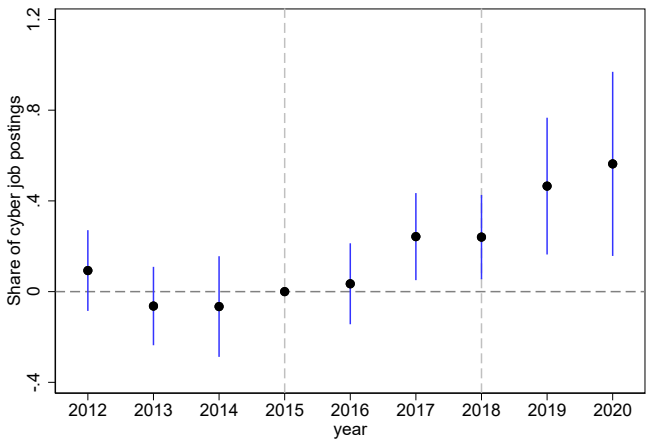
$$cyber\_share_{icjt} = \beta_1 high\ ico\ exposure_j \times SDD_t + \beta_2 high\ ico\ exposure_j \times DPA_t + \delta_{ct} + \mu_i + \varepsilon_{icjt}$$

- c: TTWA, j: 3-digit industry, t: year, i: firm.
- ε_{icjt} and ϵ_{icjt} double clustered at the 3-digit industry level and at the year level

Results

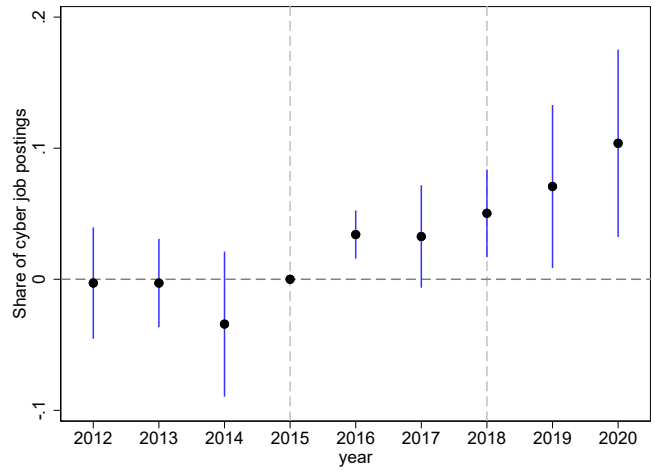
Result 1: Demand for cyber skills

(a) TTWA-level results



- SDD: Increased enforcement (2015-18): 26% ↑
- DPA 2018: Increased penalty (post-'18): 52% ↑

(b) Firm-level results

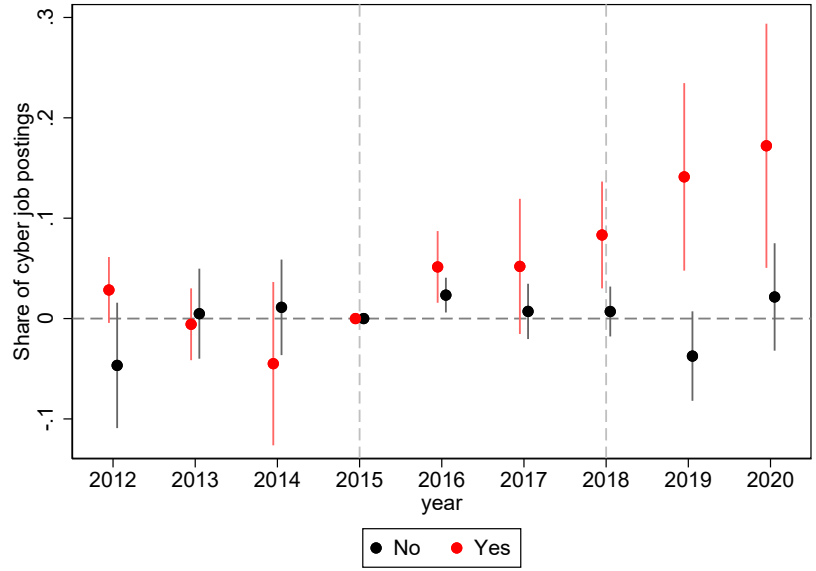


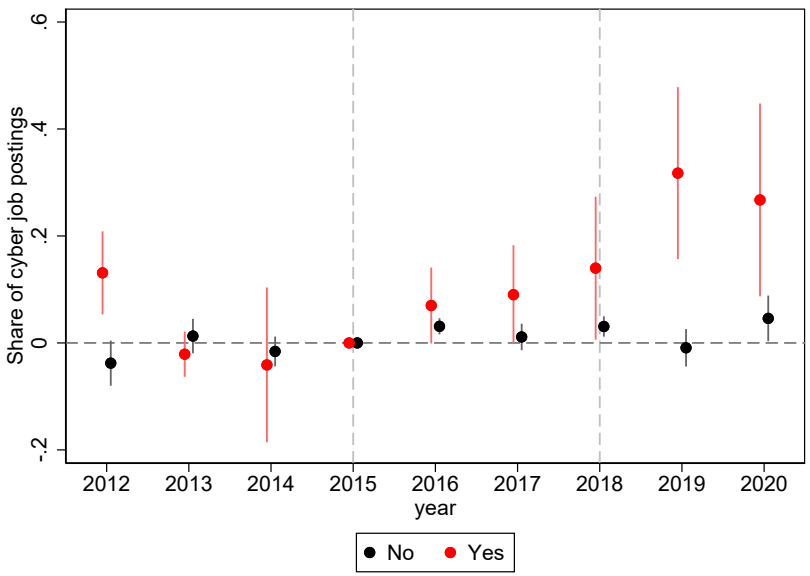
- SDD: Increased enforcement (2015-18): 37% ↑
- DPA 2018: Increased penalty (post-'18): 73% ↑

Go to table

Result 2: Differential response by firm's tech. portfolio

- Stronger response for firms investing in data harvesting skills (e.g. data mining, BI, ETL, AI, and big data).

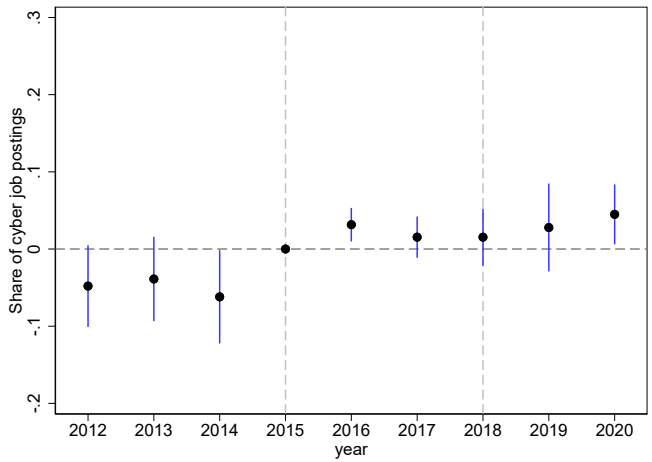




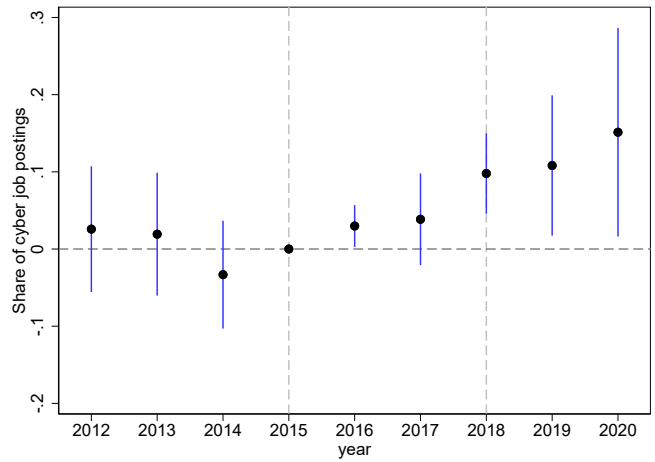
- **6 times higher**↑ among firms with cloud technologies after the passage of the DPA 2018.

Result 3: Differential response by firm's cash holding

(a) Low cash holding



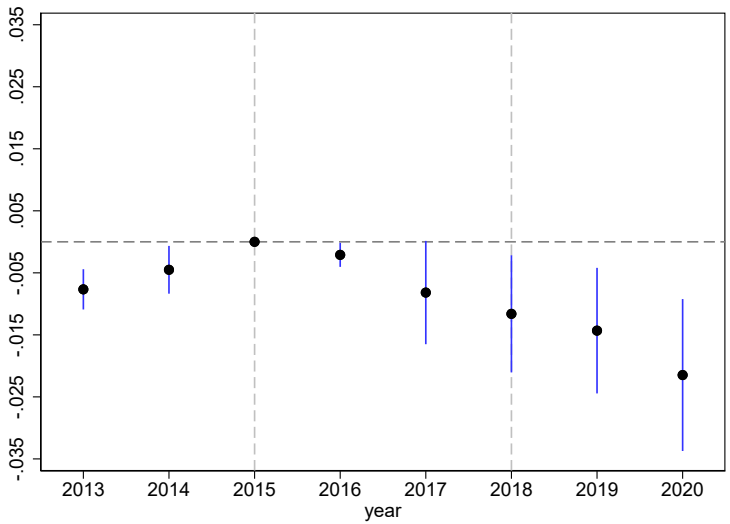
(b) High cash holding



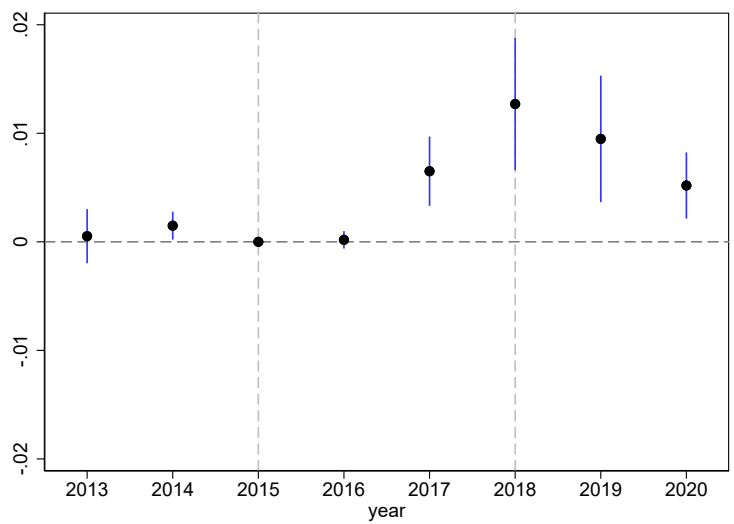
Dependent variable: % cyber job postings		
	Low	High
High ICO exposure × Increased enforcement	0.053**	0.065*
	(0.021)	(0.031)
High ICO exposure × Increased penalty	0.071*	0.135**
	(0.034)	(0.042)
Firm FE	Yes	Yes
TTWA ×*Year*	Yes	Yes
Observations	149780	124585

Result 4: Adverse effect on firm dynamics

(a) Birth rate



(b) Death rate



Post SDD

- Firm birth rate 0.6% ↓ (insig.), Firm death rate 0.9% ↑

Post DPA:

- Firm birth rate 1.4% ↓, Firm death rate 0.7%, ↑
- Economic magnitude: 12% lower birth rate , 10% higher death rate.

Concluding remarks

Key points

- Impact of enforcement and content of laws: Regulatory tools are effective in correcting underinvestment in necessary cyber skills.

Key points

- Impact of enforcement and content of laws: Regulatory tools are effective in correcting underinvestment in necessary cyber skills.

- Trade-off between enhancing cybersecurity and firm dynamism.

Key points

- Impact of enforcement and content of laws: Regulatory tools are effective in correcting underinvestment in necessary cyber skills.
- Trade-off between enhancing cybersecurity and firm dynamism.
- The negative effects of GDPR: Data access vs. data security.

Thank you

Baseline table

Dependent variable: % cyber job postings		
	TTWA level	Firm level
SDD: High ICO exposure × Increased enforcement	0.264**	0.048**
	(0.083)	(0.018)
DPA 2018: High ICO exposure × Increased penalty	0.535**	0.095**
	(0.159)	(0.038)
Mean	1.15	0.14
Industries ×*TTWA*	Yes	No
Firm FE	No	Yes
TTWA ×*Year*	Yes	Yes
Observations	144457	273488

Go back